UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

UNITED STATES OF AMERICA

v. CASE NO.: 2:21-cr-75-SPC-NPM

HERIBERTO BATISTA MONTIJO

---

**OPINION AND ORDER**[1]

Before the Court is Defendant Heriberto Batista Montijo's Motion for Pre-Trial Suppression Hearing (Doc. 28), along with the Government's response (Doc. 37) and Defendant's reply (Doc. 48). The Court held an evidentiary hearing on the Motion, at which time Defendant was present and represented by counsel. (Doc. 59). The Court reserved ruling at the hearing's conclusion but now issues this decision to explain why it denies the Motion.

## INTRODUCTION

The Motion concerns child pornography—specifically, a video of an adult male (allegedly Defendant) performing sex acts on a preteen girl ("Video"). Defendant sent the Video to another person during a chat on Facebook's instant messaging program. Facebook was monitoring the chat—or at least the files circulated. After discovering the Video, Facebook contacted the

---

[1] Disclaimer: Documents hyperlinked to CM/ECF are subject to PACER fees. By using hyperlinks, the Court does not endorse, recommend, approve, or guarantee any third parties or the services or products they provide. The Court is also not responsible for a hyperlink's availability and functionality, and a failed hyperlink does not affect this Order.

necessary authority per federal law. The Video then went to local police, who watched it without a warrant. From there, police secured two search warrants, the evidence from which led to Defendant being indicted for producing and possessing child pornography.

Defendant now seeks the Fourth Amendment's protection. He asks the Court to suppress all evidence against him because law enforcement performed an unlawful warrantless search by watching the Video. The Government defends the search under the private search doctrine, an exception to the warrant requirement.

A seemingly straightforward issue—does the private search doctrine apply here—presents tough constitutional questions that circuit and district courts have answered differently.[2] The split seems to stem from courts struggling to sync an established Fourth Amendment doctrine with today's technology used to combat the online spread of child pornography. Courts have generally applied the same seminal Supreme Court cases from the 1980s on the private search doctrine[3] to situations in which electronic service providers (like Facebook) report defendants for sending, receiving, or distributing

[2] *Compare, e.g.*, *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) and *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), *with United States v. Miller*, 982 F.3d 412 (6th Cir. 2020) and *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018).

[3] *Walter v. United States*, 447 U.S. 649 (1980) and *United States v. Jacobsen,* 466 U.S. 109, 120 (1984).

apparent child pornography. The Ninth and Tenth Circuits have found the private search doctrine inapplicable and suppressed the evidence. The Fifth, and Sixth Circuits have done the opposite, and for different reasons. The Eleventh Circuit has yet to consider the issue. Against this backdrop, the Court turns to the Motion.

## BACKGROUND

At the hearing, the Government introduced five exhibits and called two witness: (1) Raquel Morgan, a custodian of records for Facebook, Inc., and a team analyst on the Law Enforcement Response Team[4]; and (2) Patrick C. Baricelli, an FBI Task Force Officer. Defendant offered no witnesses or evidence. The relevant facts are not in dispute. Even so, the Court makes these factual findings material to the Motion based on the evidence and the parties' papers:

On March 3, 2020, two contractors on Facebook's Content Review Team confirmed a video file to show apparent child pornography under federal law. A hash value was created for it and added to Facebook's repository for later comparison. (Doc. 37-1 at 2-3).

[4] Morgan testified that she is a legal analyst for "Meta Platforms," which was previously known as Facebook, Inc. She also testified to being a custodian of records for Facebook. Defendant did not dispute her credentials or purported role, so the Court will follow suit.

A hash value "is a unique string of letters and numbers that reflects the content of an image or video file" and is created using a common algorithm like MD5. (Doc. 37-1 at 1). The series of letters and numbers are a file's digital fingerprint. Generally, electronic service providers assign a hash value to a known image of child pornography. They then scan their services for files with the same value. When they get a "match," they know the scanned file is a duplicate of the child pornography image without opening and viewing the file. And that's what happened here.

On January 23, 2021, Facebook discovered the Video in Defendant's chat and knew it contained child pornography without reopening it because the hash value matched the hash value of the video file from March 3. As explained in Morgan's declaration: "[The Video's hash value] was an exact match to an MD5 hash added to Facebook's database by a consensus of at least two contractors on March 3, 2020." (Doc. 37-1 at 1-2).

The next day, Facebook reported Defendant to the National Center for Missing and Exploited Children ("NCMEC")[5] for sending the Video on its Messenger program per federal law. *See* 18 U.S.C. § 2258A(a)(B)(1). NCMEC then generated CyberTipline Report 84991416 ("Report") using the

[5] NCMEC is a private, nonprofit organization that Congress has tasked with fielding information from electronic service providers on alleged child victimization and sharing that information with law enforcement. (Gov. Ex. 1 at 1).

information Facebook provided. (Gov. Ex. 1). The Report named Defendant[6] to be the suspect and provided his age, date of birth, verified email address, profile webpage address, and IP addresses. (Gov. Ex. 1 at 1). Four files were also listed and uploaded: the Video, Defendant's profile picture, and another video and photo that Defendant shared in the chat.[7] (Gov. Ex. 1 at 2-3).

For the Video, the Report says that Facebook assigned it an "A1" image categorization. (Gov. Ex. 1 at 2). The A1 label is based on an industry classification system that electronic service providers have been using for years to identify content in illicit material. (Gov. Ex. 1 at 5). A1 means the Video showed a prepubescent minor engaging in a sex act like intercourse or oral sex.[8] Although no one at Facebook viewed the Video in January of 2021 before it was sent to NCMEC, Facebook relied on its MD5 hash technology for the A1 label. And Morgan credibly testified that additional review was not needed because the two contractors who viewed the video in March of 2020 would not

[6] The Report names "Junior Martinez" as the suspect who is undisputedly the Defendant. (Gov. Ex. 1 at 1).

[7] The other video allegedly shows Defendant and an adolescent female hugging and kissing, and the photo shows Defendant standing behind an adolescent female with his hand over the front of her shirt and kissing her cheek. (Doc. 48-1). Facebook reported this other video and photo only to offer context to Defendant's chat. (Doc. 37-1 at 2-3).

[8] The full definition of "Sex Act" is "any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or oppose sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value." (Gov. Ex. 1 at 5).

have added the hash value to the repository if the content was not clear or certain.

The Report eventually landed on Officer Baricelli's desk. Upon receiving the Report, Officer Baricelli focused first on the Video and its A1 categorization. According to Officer Baricelli, Facebook's A1 categorization meant two things to him: (1) at some point, someone at Facebook viewed the file to confirm it contained child sexual exploitative material; and (2) the Video depicted a prepubescent minor engaging in a sex act. Officer Baricelli opened and watched the Video to verify its contents. And what he saw matched the A1 categorization. Officer Baricelli then opened Defendant's profile picture, followed by the other video and photo. He investigated more and found a complaint filed with Florida's Department of Children and Family Services ("DCF") that accused Defendant of grooming a twelve-year-old girl living with him.

Officer Baricelli eventually applied for and got search warrants for Defendant's home and car. (Gov. Exs. 4a, 4b, 5a & 5b). In applying for the warrants, Officer Baricelli detailed the Video's content and described the DCF complaint. (Gov. Exs. 4a & 5a). He did not mention the other video or photo that Facebook provided.

The police eventually seized enough evidence for Defendant to be indicted on three counts of producing and possessing child pornography. (Doc. 1). This Motion followed, the merits of which are addressed next.

## DISCUSSION

Defendant argues the Court should exclude all evidence against him because Officer Baricelli violated his Fourth Amendment rights when he watched the Video without a warrant. The Government responds that Officer Baricelli replicated Facebook's prior private search, so the Fourth Amendment did not require a warrant. It also says that Defendant had no reasonable expectation of privacy in the Facebook chat and the good-faith exception to the exclusionary rule applies. The Court tackles each argument.

### A. Private Search Doctrine

The Fourth Amendment protects individuals against the government performing unreasonable searches and seizures. U.S. Const. amend. IV. The government usually needs a warrant before it may search a person or his effects. A warrantless search is invalid unless an exception applies to the warrant requirement. *See Katz v. United States*, 389 U.S. 347, 357 (1967). The exception the Government relies on here is the private search doctrine.

The Fourth Amendment protects individuals from government actors, not private ones. A private party thus may conduct a search that would be unconstitutional if the government did it. From this principle comes the

private search doctrine. When a private party acts on its own accord and provides evidence against a defendant to the government, the police need not "avert their eyes."[9] *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971). So the Fourth Amendment allows police to replicate a prior private search provided it stays within the same parameters. *See United States v. Sparks*, 806 F.3d 1323, 1334 (11th Cir. 2015) ("So once an individual's expectation of privacy in particular information has been frustrated by a private individual, the Fourth Amendment does not prohibit law enforcement's subsequent use of that information, even if obtained without a warrant." (citations omitted), *overruled on other grounds by United States v. Ross*, 963 F.3d 1056 (11th Cir. 2020).

The Supreme Court formalized the private search doctrine in two cases: *Walter* and *Jacobsen*. Both considered a warrantless government search after a private party gave the government information for its investigation. Together, the cases determined that a prior private search excuses the government from getting a warrant to repeat the search but only when the government's search does not exceed the scope of the private one. Because *Walter* and *Jacobsen* are the formative cases on the private search doctrine, the Court starts with them.

[9] It is undisputed that Facebook is a private entity that acted independently of the Government and without the Government's knowledge or participation.

In *Walter*, a dozen sealed packages containing hundreds of boxes of eight-millimeter films "depicting homosexual activities" were delivered to the wrong corporate address. 447 U.S. at 649, 651 (1980). Employees opened each package and examined the boxes with suggestive drawings on one side and explicit descriptions of the contents on the other. An employee opened one or two boxes and tried without success to view the film by holding it up to the light. The FBI was called, who viewed the films without a warrant. Indictments followed.

The Supreme Court's plurality opinion concluded the agents exceeded the scope of the private search because they had to view the films—when no employee had done so—to know whether the defendants committed any crime:

> It is perfectly obvious that the agents' reason for viewing the films was to determine whether their owner was guilty of a federal offense. To be sure, the labels on the film boxes gave them probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction and were not mentioned in the indictment. Further investigation—that is to say, a search of the contents of the films—was necessary in order to obtain the evidence which was to be used at trial.
>
> . . . .
>
> Prior to the Government screening [of the films] one could only draw inferences about what was on the films. The projection of the films was a significant expansion of the search that had been conducted

> previously by a private party and therefore must be characterized as a separate search.

447 U.S. at 654, 657 (footnote omitted).

Fast forward four years to *Jacobsen*, where the Supreme Court again undertook the private search doctrine. 466 U.S. 109 (1984). There, Federal Express employees opened a damaged package to find a tube holding zip-lock bags, the innermost of which contained a white powder. Rather than opening the bag with the powder, the employees called the DEA. When the agents arrived, they removed the tube from the box, removed the plastic bags from the tube, opened each bag, removed some powder, and fielded tested it to confirm it was cocaine.

The Supreme Court addressed whether the private search doctrine saved the warrantless search. The Court's consideration was twofold: (1) how much the agents' actions led to them learning new information the employees did not uncover; and (2) how far the agents' investigation intruded on the package owner's privacy interest beyond the employees' intrusion. The Court concluded the agents gleaned no new information than what the employees told them by removing the plastic bags from the tube and visually inspecting the contents, so they did not exceed the scope of the private search. *Id.* at 120. It also found the employees infringed on the owner's expectation of privacy when they opened the package and invited the agents to examine the contents. *Id.* at 121.

As to the chemical field test, the Supreme Court determined it was not a search under the Fourth Amendment because "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest." *Id.* at 123. At bottom, the Court found "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of the private conduct." *Id.* at 126.

Applying the private search doctrine here as delineated in *Walter* and *Jacobsen*, the Court finds the government search did not exceed the scope of Facebook's prior search because Officer Baricelli did not learn new, critical information needed to get a warrant. Nor did the government expand on Facebook's prior search when Officer Baricelli viewed the Video even though no one at Facebook had done so on this occasion before reporting to NCMEC. And here is why.

To start, Defendant makes much about the Government not providing evidence on the contractors' identities and how Facebook found the offending files. But Facebook and its contractors are private persons. So the who and how Facebook searches its programs do not lessen the private search doctrine's application here.

Having settled that, the record is undisputed that when Officer Baricelli watched the Video, he knew it would show a prepubescent minor engaged in a

defined type of sex act. He knew so because the Report said that Facebook gave the Video an A1 category. Yet Defendant argues Officer Baricelli learned more from watching the Video than Facebook provided and faults him for including detailed information in his search warrant affidavits. This argument misses the mark.

By watching the Video, Officer Baricelli did not learn new, critical information about the unlawful content in the Video. He just observed how the A1 definition applied. The Report included Facebook's A1 categorization and its parameters. Officer Baricelli's affidavits tracks the A1 categorization with details on the label's accuracy. For example, the affidavits in one paragraph detail an adult male attempting genital-genital intercourse with a prepubescent girl and switching to performing oral sex on her. (Gov. Ex. 4a at 7; Gov. Ex. 5a at 7). Officer Baricelli was merely more thorough in describing the illicit material than the Report, and his thoroughness does not violate the Fourth Amendment. For this point, the Court follows the Eleventh Circuit's decision in *United States v. Simpson*, 904 F.2d 607 (11th Cir. 1990).

There, the defendant moved to suppress child pornography tapes that Federal Express employees discovered in a package, watched, and reported to authorities. A prosecutor and FBI agent later viewed the same tapes. The defendant moved to suppress, arguing the Government exceeded the employees' prior private search. The Eleventh Circuit disagreed:

> The box's contents had already been examined, their illicit character had been determined, and they were open for viewing by the time the Assistant United States Attorney and the F.B.I. Agent arrived on the scene. Their search of the box and videotapes did not exceed the scope of the prior private searches for Fourth Amendment purposes simply because they took more time and were more thorough than the Federal Express agents.

904 F.2d at 610. Facebook used its MD5 hash technology to label the Video's illicit content as A1. Officer Baricelli viewing the Video did not exceed Facebook's prior private search just because he recorded more details. *See generally Rogers v. Sec'y, Dep't of Corr.*, No. 8:17-CV-2680-T-33SPF, 2019 WL 2646544, at *6 (M.D. Fla. June 27, 2019) (finding a § 2255 petitioner did not "identif[y] any clearly established federal law holding that when a private searcher views at least one image on a disk and tells police that the disk contains contraband, police exceed the scope of the private search by viewing other images on that same disk"), *aff'd,* 829 F. App'x 437 (11th Cir. 2020).

This case is also unlike *Walter* because Facebook's A1 categorization told Officer Baricelli he would see a preteen minor engaged in intercourse or oral sex—and that's what the Video showed. He did not need to watch the Video to know Defendant committed a federal crime. Facebook told him so through the A1 label. And recall in *Walter* that no employee viewed the films and the government had to use the exterior covers to know what the films' content. But Facebook used its MD5 hash technology to know it discovered a duplicate file

of apparent child pornography that two contractors previously identified. (Doc. 37-1 at 1).

This case is not as if a private citizen stumbled across a child pornography image on a laptop or cell phone and gave the device to law enforcement who then searched the device's entire contents. Rather, Facebook's contractors, who are trained on what constitutes child pornography under federal law, verified the illicit content of a duplicate file of the Video. And Officer Baricelli viewed only that single Video that Facebook provided. In doing so, he reviewed the same information discovered during the private search. Under these facts, Officer Baricelli did not need to avert his eyes from the Video when he received the Report. *See Coolidge*, 403 U.S. at 489. The Court thus finds the private search doctrine applies to justify the warrantless search of the Video.

In reaching this decision, the Court is mindful of the legal split on this issue.[10] It also recognizes that the Ninth Circuit in *Wilson* recently decided a

[10] *Compare United States v. Wilson*, 13 F.4th 961, 964 (9th Cir. 2021) (holding that the private search doctrine did not justify the government's warrantless search of the defendant's email attachments provided through NCMEC's CyberTipline) and *United States v. Ackerman*, 831 F.3d 1292, 1306 (10th Cir. 2016) (holding NCMEC's search of the defendant's email and images exceeded the scope of AOL's search because AOL learned only that a single image had a hash-value match, but the NCMEC analyst viewed the entire email, so the analyst's search disclosed more information), *with United States v. Miller*, 982 F.3d 412 (2020) (holding hash value matching does not implicate the Fourth Amendment under the private search doctrine); *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018) (finding Microsoft determined that hash values of files the defendant uploaded matched the hash values of known child pornography images, so the government could rely on that private search to view the files without violating the defendant's constitutional rights); *United States v. Bonds*, 5:21-

factually similar case and reached the opposite conclusion. But the Eleventh Circuit has not yet weighed in whether the Fourth Amendment prohibits an officer from opening and reviewing the files after a private party has determined that the files' hash values matched known child pornography images in its database. So the Court has anchored its analysis to the original precedents announced in *Walter* and *Jacobsen* and applied those principles to deny Defendant's motion.

**B. Reasonable Expectation of Privacy**

The Court further finds that Defendant did not have a reasonable expectation of privacy in his Messenger chat or the Video. A defendant can only invoke the Fourth Amendment's protection where he has a legitimate expectation of privacy in the item searched. *See Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978). The privacy interest is both subjective and objective: a defendant must show he subjectively expected privacy, and the expectation is one that society recognizes as reasonable. *See United States v. Ford*, 34 F.3d 992, 995 (11th Cir. 1994) (citation omitted). But an individual's expectation of

---

cr-43-KDB-DCK, 2021 WL 4782270, at *3 (W.D.N.C. Oct. 13, 2021) (denying a motion to suppress because the officer obtained information only learned during a private search of the defendant's Google Drive account); *Matter of Search of Encrypted Data Provided by Nat'l Ctr. for Missing & Exploited Child. for Nineteen Related Cyber Tipline Reps.*, No. 20-SW-321 (ZMF), 2021 WL 2100997, at *7 (D.D.C. May 22, 2021) (denying a search warrant because Google's private search revealed that the files on Google Drive were a hash match to known child pornography; "[t]he Fourth Amendment should not be used to place unnecessary and wasteful roadblocks between a private actor's voluntary disclosure of criminal activity and the government's lawful use of such information.").

privacy is not always forever. A common example of when an expectation of privacy is frustrated is when information is revealed to a third party. *See* *Jacobsen*, 466 U.S. at 117 ("It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information[.]" (citation and footnote omitted).

Here, Defendant revealed the Video's content not only to his intended Messenger recipient, but also to Facebook. He risked that both would turn the Video over to the Government. Although the recipient did not, Facebook did. And the Court need look no further than Facebook's written policies to know it gave Defendant fair warning of that risk.

Facebook's Terms of Service govern a user's use of Messenger, and all users, including Defendant, must agree to the terms upon joining Facebook. The Terms of Service reflect Facebook's strong stance against users abusing its services to spread unlawful and toxic content:

> We employ dedicated teams around the world and develop advanced technical systems to *detect* misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or

> conduct like this, we will take appropriate action – for example, offering help, removing content, removing or restricting access to certain features, disabling an account, or *contacting law enforcement*.
> . . . .
>
> And we develop *automated systems* to improve our ability to *detect* and remove abusive and dangerous activity that may harm our community and the integrity of our Products.

(Gov. Ex. 2 at 2-3 (emphasis added)). The Terms of Service also permit Facebook to store, copy, and share any photo the user posts. (Gov. Ex. 2 at 7).

Complimenting the Terms of Service are Facebook's Community Standards that offer written guidelines on what users may share on Facebook. (Gov. Ex. 2 at 12). The Community Standard titled, "Child Sexual Exploitation, Abuse and Nudity," applies here. (Gov. Ex. 6). It reads, "We do not allow content that sexually exploits or endangers children. When we become aware of apparent child exploitation, we report it to the National Center for Missing and Exploited Children (NCMEC), in compliance with applicable law." (Gov. Ex. 6 at 1; *see also* Doc. 37-1 at 1). It then outlines types of content involving illicit material that cannot be posted. (Gov. Ex. 6 at 2-3).

Under the Terms of Service and Community Standards, Facebook warned Defendant he risked being reported to law enforcement or NCMEC if Facebook discovered that he sent, received, or distributed apparent child pornography. To the extent Defendant argues that Facebook does not

explicitly state it will monitor a user's Messenger chats or images shared in it, that outcome is reasonably implied with the caution that Facebook will use technology to detect the misuse of its services. (Gov. Ex. 2 at 2). And how can Facebook "detect" if it does not "monitor" in some way? Even if Defendant believed that his communications in Messenger were private, society is not prepared to recognize that belief as reasonable given Facebook's Terms of Service and Community Standards. In the end, Defendant lost any expectation of privacy in the Video once he hit send. *See United States v. Odoni*, 782 F.3d 1226, 1238 (11th Cir. 2015) ("An individual does not have a reasonable expectation of privacy in an object to the extent the object has been searched by a private party." (citation omitted)). Without a reasonable expectation of privacy, Officer Baricelli did not violate his Fourth Amendment rights when he watched the Video, and any privacy was waived by Facebook's prior search.[11]

**C. Good-faith exception**

Even if Defendant had a reasonable expectation of privacy and the private search doctrine does not apply, the Court still denies the Motion under

[11] Defendant provided no evidence to show his subjective expectation of privacy in his Messenger chat or the Video. *See generally United States v. Devers*, No. 12-CR-50-JHP, 2012 WL 12540235, at *2 (N.D. Okla. Dec. 28, 2012) ("[U]nless the defendants can prove that their [F]acebook accounts contained security settings which prevented anyone from accessing their accounts, this court finds their legitimate expectation of privacy ended when they disseminated posts to their 'friends' because those 'friends' could use the information however they wanted–including sharing it with the government").

the good-faith exception. To discourage police from violating the Fourth Amendment, courts have created the remedy of excluding "improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009). But "exclusion 'has always been our last resort, not our first impulse.'" *Id.* at 140 (citation omitted). The exclusionary rule's "sole purpose . . . is to deter future Fourth Amendment violations." *Davis v. United States*, 564 U.S. 229, 236-37 (2011) (citations omitted). Courts must thus engage in a "rigorous weighing of [exclusion's] costs and deterrence benefits" to determine whether exclusion is warranted." *Id.* at 238. And the good-faith exception comes into that analysis. Under the exception, courts do not exclude evidence when law enforcement acts, as here, in "objectively reasonable reliance upon a statute authorizing" the search. *Illinois v. Krull*, 480 U.S. 340, 349 (1987) ("The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant.").

Officer Baricelli acted in objectively reasonable reliance on Facebook's statutory reporting requirements to view the Video. *See* 18 U.S.C. § 2258A; *see also United States v. Ackerman*, 804 F. App'x 900, 905 (10th Cir. 2020) (finding that the good-faith exception applied when NCMEC searched the defendant's email in good faith under § 2258A). Electronic service providers like Facebook

must report to NCMEC's CyberTipline after it obtains "actual knowledge" of any apparent child pornography. 18 U.S.C. § 2258A(a)(1)-(2). They can even be fined if they do not do so. *Id.* § 2258A(e). NCMEC too has statutory obligations. It must maintain the CyberTipline and forward every report it receives to law enforcement. *Id.* § 2258A(a)(1)(B) & (c). Congress has also permitted NCMEC to receive and review the illicit material without breaking the law. *Id.* § 2258A(c).

Under this statutory scheme, Officer Baricelli acted in objectively reasonably reliance on Facebook's and NCMEC's legal obligations to watch the Video. *See generally United States v. Leon*, 468 U.S. 897, 918 (1984) (stating the exclusion of evidence is an "extreme sanction" that "should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule"). Facebook was a reliable source who reported the Video per the law. And this wasn't Facebook's first report to NCMEC. For over fifteen years, Facebook has routinely notified NCMEC of child sexual exploitation it has discovered. In 2020 alone, for example, Facebook submitted over 20 million reports. (Doc. 37-2 at 2). Nor was this Officer Baricelli's first report from NCMEC. And Officer Baricelli, who has been trained on child sexual exploitation investigations and completed continuing education on the topic, is experienced with NCMEC and even reports from Facebook. He credibly testified that he has received over 300

CyberTipline reports from NCMEC and that he has found Facebook's categorization of apparent child pornography to be reliable and accurate.

In conclusion, Officer Baricelli reasonably relied on Facebook's and NCMEC's statutory duty to report apparent child pornography and voluntarily provide the incriminating evidence to watch the Video. The Court thus alternatively denies Defendant's Motion on the good-faith exception.

Accordingly, it is now

**ORDERED:**

Defendant Heriberto Batista Montijo's Motion for Pre-Trial Suppression Hearing (Doc. 28) is **DENIED**.

**DONE AND ORDERED** in Fort Myers, Florida on January 10, 2022.

SHERI POLSTER CHAPPELL
UNITED STATES DISTRICT JUDGE

Copies: Counsel of Record